View metadata, citation and similar papers at core.ac.uk
brought to you by CORE
provided by The Journal of Social Media in Society

The Journal of Social Media in Society
Spring 2019, Vol. 8, No. 1, Page 271-278
thejsms.org

ESSAY

Facebook Under Attack? Privacy – Europe's Way of Waging War on U.S. Giants?

Charlotte Gerrish* and Samya Idi
Gerrish Legal
*Corresponding author: cg@gerrishlegal.com and @gerrish_legal

With the latest focus across Europe and globally on data protection and privacy issues, not least in light of the General Data Protection Regulation (GDPR) (EU) 2016/679 which came into force in all member states of the European Union on 25th May 2018, social media sites have come under scrutiny for their data protection practices.

Keywords: Europe; social media; data protection; privacy; law; EU; GDPR; Cloud Act; Politics; US

As soon as the General Data Protection Regulation (GDPR) came into effect, Facebook, along with Google, was immediately accused of failing to comply with European Data Protection laws. Facebook, the U.S. giant has been making headlines for months. The first was due to its implication in a massive personal data scandal: the Cambridge Analytica Saga.

A UK based analytics firm, Cambridge Analytica was alleged of using data of up to 87 million Facebook users to influence the outcome of the 2016 U.S. presidential elections and the Brexit vote. The affair shed light on the significant impact of Facebook on both private and public spheres. In Europe, the scandal particularly raised concerns on the role played by social media in our democracies. The gravity of the situation led Facebook CEO, Mark Zuckerberg, to testify before the European Union Parliament on May 22, 2018.

The European Union has been very active in chasing the data breaches that the social media giant has initiated. Over the past months, courts, supervisory authorities and lawmakers aligned to address and publicly condemn the misuse of personal data by

Facebook. This phenomenon raises an important question: is data protection a new way for Europe to wage war on US Giants?

This article will address the role played by both supervisory authorities and the Court of Justice of the European Union (CJEU) in the protection of personal data (I), and will assess the U.S. Cloud Act as a counter attack on an increasing scrutiny against U.S. giants, such as Facebook (II). The cases are developing rapidly and decisions are being handed down often, so opinions can shift frequently. This article represents the law as at January 2019.

The EU at War with U.S. Social Media Giants

Without question the impact of social media on our daily lives has been phenomenal over the last decade, but as a consequence of this, the multinational corporation, Facebook, has been the main target of a European war against privacy violations. Data Protection Authorities (A) and the CJEU (B), have formed a united front in this fight.

Data protection authorities, the soldiers of a long-lasting war. Back in 2014, Data Protection Authorities based in France, Spain, Germany, the Netherlands and Belgium created a consortium to analyse the changes that Facebook had made to its privacy and user policy. In France, the French Data Protection Authority (the "CNIL") observed that Facebook collected personal data of internet users on a mass scale in order to display targeted advertising. The CNIL also discovered that Facebook collected data related to internet users' activity on third-party websites, via the "datr" cookie, all without the users' knowledge or consent. This resulted in a fine of €150,000 being ordered by the CNIL against Facebook back in May 2017.

Also in May 2017, the Data Protection Authority in the Netherlands (known as the "Autoriteit Persoonsgegevens") confirmed that Facebook was in breach of Dutch data protection law, following an investigation that it conducted into the processing of personal data of 9.6 million Dutch Facebook users. The Dutch Data Protection Authority noted specifically that Facebook failed to give users sufficient information about the use of their personal data, and also used sensitive personal data from users without their explicit consent, including processing data relating to sexual preferences to show targeted advertisements.

In Spain, the Spanish Data Protection Authority conducted preliminary investigations into Facebook's privacy policy and terms of use and commenced two infringement procedures. The procedures, considering the results of the investigations, were based on alleged infringement of the provisions of Spanish data protection law.

In Belgium, a 3 year-long ongoing battle between Facebook and the Belgian Data Protection Authority (the "Commission Pour la Protection de la Vie Privée", or "CVPV") came to conclusion in February 2018. The Belgian Data Protection Authority's audit revealed that even if you have never visited Facebook's page, Facebook is nonetheless able to follow your online movements without you knowing (and without your consent), due to the pixels that Facebook has integrated into more than 10,000 websites.

The Belgian Courts considered that Facebook was in breach of Belgian Privacy Laws. As such, the Belgian judges considered that it was appropriate to accept the Belgian Data Protection Authority's request and imposed a strict sanction on Facebook, which consisted of destroying all personal data unlawfully obtained and publishing the entire judgment of 84 pages on its website. Judges also provided for additional punishment in the event that Facebook refuses to comply with the terms (which are common in civil law jurisdictions), including a penalty fee of €250,000 per day of delay to comply with the judgment, up to a maximum of €100 million.

More recently, two European Consumer Rights organisations None Of your Business (Noyb) and La Quadrature du Net filed the complaints against Facebook and Google before the CNIL, arguing that these tech companies violated one of the key rules of the GDPR: consent. NOYB pointed out that users were not provided clear information and the technical sign up process would essentially force users to provide their consent to the new terms, even if they did not really wish to do so. The CNIL reviewed these complaints and agreed with the pressure groups that the difficult to understand privacy agreements and "take it or leave it" agreement options meant consent could not possibly be considered valid under the GDPR. As a result of this complaint, in January 2019, the CNIL issued a record breaking fine in 2019 of €50 million, to Google, which it has stated it will appeal.

Several EU Member States, including France, Belgium, Germany (Hamburg) and Austria were invited to fine Facebook and Google up to the maximum amount of 4 percent of their global annual revenue. Going forward, EU regulators will have to state their

interpretation of the GDPR in the context of this case, which is great news for lawyers and their clients (given the new and uncertain nature of the GDPR) but is a huge onus on these tech giants to go forward defending their companies whilst shaping privacy law for the future. This battle launched by European Data Protection Authorities to make multinational companies accountable, has been supported by the CJEU.

The CJEU, chief commander of the war against privacy rights violations. The CJEU has had a constant watchful eye over the actions of social media sites and search engines in relation to personal data. In 2014 it gave clear instructions on the right to be forgotten: EU citizens are entitled to request that their personal data is erased from search engines and social media sites if the information is incorrect, inappropriate or excessive (Judgement of 13 May 2014, *Google Spain SL and Google Inc v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González,* C-131/12). This right is now legislated in the GDPR (*Article 17(2)*), however, it must always be considered in relation to the right of freedom of expression and access to public information. This means there is a contentious balancing act for adjudicators to perform.

One of the most infamous cases on data protection before the CJEU was when it had to deal with the case brought by Maximillian Schrems against Data Protection Commissioner (Judgment of 6 October 2015, *Maximillian Schrems v Data Protection Commissioner*, C-362/14). The case was filed before GDPR came into force and was based on the old EU Directive.

Mr. Schrems, an Austrian law student, filed a complaint before the Irish privacy supervisory authority regarding the transfer of his personal data to servers based in the U.S, on the grounds that the U.S. did not provide an adequate level of protection against surveillance (according to Edward Snowden's revelations regarding NSA files). The Irish privacy supervisory authority rejected the complaint, arguing thanks to the Safe Harbour decision, the U.S. was considered to be a territory providing an adequate level of protection in respect of personal data transferred there from the EU.

The Irish privacy supervisory authority's decision was brought before the High Court of Ireland, which referred the matter to the CJEU. In its noteworthy decision, the CJEU held that supervisory authorities in charge of privacy issues are entitled, under the Charter of Fundamental Rights of the European Union and the EU directive, to challenge

the level of protection of the personal data transferred and suspend the transfer of the data of Facebook's European subscribers, despite the existence of the Safe Harbour, if the level of protection is not adequate. The power given by the CJEU to supervisory authorities, through this decision, confirms the important role played by authorities in the protection of personal data.

Further, just few days after the GDPR came into effect, on 5th of June 2018, the CJEU rendered an enlightening decision on the role of the administrators of Facebook fan pages in processing data (Judgment of 5 June 2018, *Wirtschaftsakademie Schleswig-Holstein*, C-210/16) against a German company which offered educational services through their Facebook fan page. Facebook, through the medium of cookies, would collect and process the personal data of visitors to the fan page, which allowed the administrators of the fan page to personally identify those visitors.

The Independent Data Protection Authority in Germany argued that visitors of the Facebook fan page were not informed of such processing. The Independent Data Protection Authority in Germany therefore ordered for the fan page to be deactivated, and unsurprisingly, the German Company appealed the decision before the German administrative courts. According to the German company, the German courts had no jurisdiction to hear the case, since the only "processing party" was Facebook, which is a U.S. registered company. The German company argued that proceedings should only be brought against Facebook before the American courts.

On the basis of the German company's arguments, the case was referred to the CJEU, which was tasked with interpreting the pre-GDPR law on data protection (since the case was issued before the GDPR came into force). The CJEU expressly stated that administrators of fan pages on Facebook were co-controllers of the personal data processed by Facebook, as the platform was beneficial to them. Consequently, fan page administrators must be held jointly responsible with Facebook US and its European subsidiary (Facebook Ireland) for all personal data processing on the Facebook page. One of the key principles of this decision is the empowerment given, once again, by the CJEU to supervisory authorities tasked with overseeing privacy across the EU. Indeed, the CJEU further stated that supervisory authorities based in one Member State have direct jurisdiction to assess the lawfulness of data processing by a third party based in

another Member State which breaks down the administrative burden in enforcing cross border privacy violations as within the European Union.

There is also limits to the EU Courts' ability to protect personal data. While it has championed the right to be forgotten and the possibility for citizens to request data about them is deleted in previous cases, it seems now in an appeal case by Google that the CJEU will accept that the right to be forgotten only exists in the EU, and Google can continue to display the information in the rest of the world. This is following the CNIL fining Google €150,000 for deleting data at the request of an EU citizen only in the EU, and not world-wide. Advocate General Maciej Szpunar's has commented that to force Google to delete the data everywhere in the world could have unintended consequences of EU citizens losing the ability to access information based on decisions made in countries outside the EU, and lead to extreme censorship in some countries.

Facebook is clearly within the sights of the EU as it fights to protect its citizens' personal data. The U.S. has not been irresponsive to this war waged against its tech giants, especially given the recent enactment of the Cloud Act.

The U.S. CLOUD Act: a counter attack?

Two months before the GDPR came into force, on 23rd March 2018, U.S. President Donald Trump signed the Clarifying Overseas Use of Data Act, also known as the CLOUD Act. The Act, which addresses internet privacy issues, a hot topic at the moment, was passed in the most discrete of ways.

As part of the US$1.3. trillion government spending bill, the CLOUD Act amended the privacy provisions provided by the 1986 Stored Communications Act (SCA). This also took place just one month after the U.S. Supreme Court Justices were tasked with the Microsoft Ireland case. Sceptics feel that this is hardly a coincidence.

One of the questions raised in the Microsoft Ireland case was whether data located outside of the U.S. could be subject to a warrant from the U.S government. The CLOUD Act responded clearly to this question, relieving the Justices of the Supreme Court of the burden of deciding on the issue.

Indeed, the CLOUD Act states that data detained by services providers which are located outside of the U.S must be disclosed on request (to be codified at 18 U.S.C. § 2713). The CLOUD Act also provides that, in the event that such requests conflict with the law of

foreign governments, it is for the Courts analyse the different factors as to whether the data can be disclosed or not (CLOUD Act § 103(b), to be codified at 18 U.S.C. § 2703(h)). These provisions of the CLOUD Act are in total conflict with EU law and the GDPR, which forbids transfer of data outside of the European Union, unless certain conditions are respected.

Indeed, Article 48 of the GDPR says specifically that Court orders requesting the transfer of data outside of the EU, are only accepted on the ground of an international agreement, such as via a mutual legal assistance treaty. The EU and the U.S are not bound by an international agreement addressing this issue. Thus, a U.S. warrant requesting the transfer of data held in the EU is deemed likely to violate EU law. Is the CLOUD Act a demonstration by the U.S of its response to repetitive attacks by the EU against its companies?

It is clear that the CLOUD Act drastically reduces privacy rights and shows that the U.S government has taken a stance in direct opposition to the principles of the GDPR, and the European lawmakers' intention to create a high standard of privacy rights.
The CLOUD Act is not just contrary to EU principles, but it also appears to impact EU countries on a more local level – for example, the French Law "Blocking Statute" acts a shield against discovery procedures or "fishing expeditions" by Courts and authorities, which are forbidden in France (or at least extremely limited pursuant to French litigation rules).

By giving U.S law enforcement authorities extensive powers, such as allowing them to bypass the EU law privacy protections, it seems highly likely (at least from a European perspective) that the CLOUD Act is evidence of a political will of the U.S. government to reaffirm its sovereignty over international standards and tendencies.
The CLOUD Act should not be taken as a mere response to the EU's data protection regulation. The CLOUD Act could also have the effect of encouraging other countries to legislate in a similar way, to protect their internal and commercial interests, and diminish the scope of the EU's will to put data protection in the agenda on a global basis.

Conclusion

The mass of questions that Facebook CEO Mark Zuckerberg was asked during his hearing before the EU Parliament, demonstrates that European lawmakers are willing to

hold Facebook and other multinational companies accountable, when they are dealing with personal data on a large scale. Indeed, throughout the years, privacy rights were strengthened, due to the increasing data beaches that occurred via social media. However, the EU is facing new challenges with responsive jurisdictions such as the United States. The GDPR, as a great move towards transparency and the respect of privacy rights, is of course not welcomed everywhere. Perhaps this means that a privacy war has indeed been waged, and it is clear that neither side will go down without a fight – perhaps the best way forward is to enter into a Peace Treaty where all sides cooperate with each other to create international tools, in order to implement standards of data protection and ensure that privacy rights are adhered to on an international scale.

References

Daskal, J. (2018). Microsoft Ireland, the CLOUD Act, and International Lawmaking 2.0. Stanford Law Review Online 71, 9-16.

Greenfield, P. (2018, March 26). The Cambridge Analytica files: The story so far. *The Guardian.* Retrieved from https://www.theguardian.com/news/2018/mar/26/the-cambridge-analytica-files-the-story-so-far

Hern, A. (2018, May 25). Facebook and Google targeted as first GDPR complaints files. *The Guardian.* Retrieved from https://www.theguardian.com/technology/2018/may/25/facebook-google-gdpr-complaints-eu-consumer-rights

Notes, Funding and Acknowledgements

The author declares no funding sources or conflicts of interest. This article is for information purposes only and does not constitute definitive legal advice.

Online Connections

To follow Charlotte Gerrish on social media: Twitter - @gerrish_legal, LinkedIn - www.linkedin.com/in/charlottegerrishlegal